정 보 보 호 학 회 지
제23권 제6호, 2013. 12

인터넷 주소 등록기관을 활용한 피싱 URL 분석 연구

강 지 윤*, 조 은 정**, 이 시 형***

요 약

전자금융서비스 활용이 급격히 증가함에 따라 (예) 인터넷 자동이체, 조회) 이를 악용한 범죄 역시 증가하고 있다. 특히, 금융서비스 제공자를 사칭한 문자 메시지나 이메일을 전송하여 실제와 유사한 허위 URL에 접속하도록 유도하는 파밍 공격이 이러한 범죄의 대표적인 예이다. 이에 따라 다양한 대응방안들이 등장했지만 이들은 공통된 취약점이 존재한다. 기존 사이트들의 적극적인 참여가 필요하며, IP주소의 위조에 취약하다는 것이다. 이와 같은 문제점을 해결하기 위해 본 논문은 인터넷 주소 등록기관을 통한 URL 검증 기법을 제안한다. 제안된 기법에서는 주어진 URL의 등록기관 및 국가를 검증하여 악성 사이트로 유도하는 URL을 탐지한다. 제시된 방법의 정확도를 평가하기 위해 인터넷 금융과 관련된 총 44개 URL의 등록기관 및 국가를 검증해 보았으며, 90%이상의 정상 사이트 및 80% 이상의 비정상 사이트를 정확히 판별해 낼 수 있음을 확인하였다.

Ⅰ. 서 론

정보망 보급의 일반화와 스마트 기기 사용의 급증으로 인해 전자금융서비스에 대한 접근이 훨씬 용이해졌다. 2012년 1분기 말 전자금융서비스 이용율은 최고 8,015만 명을 기록하였다 [1]. 이와 같은 사용률 급증에 따라 를 악용한 피해사례와 피해 금액 또한 증가 추세에 있으며, 이중 30% 이상의 피해사례가 정상 사이트를 가장한 허위 사이트로 유도하는 파밍(pharming) 공격이다.

이러한 문제를 방지하기 위해 다양한 검증 기법들이 제안되었다. 이중 대표적인 두 가지 방법은 (i) 접속지로부터 전자서명(digital signature)을 받아 정상 사이트임을 검증하거나 [2], (ii) 피해가 보고된 허위 주소의 목록을 만들에 접속지 주소를 이와 비교함으로써 악성 여부를 확인하는 것이다 [2,4]. 하지만 전자서명은 접속지가 제 3의 기관에 미리 등록된 경우만 인증 가능하며, 허위 주소의 목록 역시 접속지가 목록에 미리 등록된 경우만 악성 여부를 확인 가능하다. 두 기법의 단점을 보완하기 위해 검색엔진을 통해 접속지의 호스트네임을 확인하는 방법이 제안되었으나 [3], 접속지의 IP주소 변조는 확인하지 못한다. 즉, 접속지의 호스트네임이 위조되지 않았더라도, DNS 스푸핑 공격 [2] 등을 통해 최종 접속지의 IP주소가 변조된다면, 사용자는 여전히 피싱 사이트에 접속하게 된다.

우리는 이러한 기존 솔루션의 문제점을 보완하는 인터넷 주소 등록기관을 통한 악성 URL 탐지 기법을 제안한다. 제안하는 방식은 인터넷 주소 등록기관의 WHOIS 데이터베이스로부터 접속지의 주소 및 등록 기관을 확인함으로써 주어진 URL의 진위 여부를 판별한다. WHOIS 데이터베이스는 인터넷 주소 등록기관에 의해 관리되므로 등록 및 정보 갱신에 소요되는 비용이 낮으며, 최종 접속지의 IP 주소를 검증하므로, IP 주소의 변조 여부도 검증 가능하다. 제안된 방식은 총 12개의 정상 URL (12개 은행 사이트) 및 32개 악성 URL을 대상으로 평가되었으며, 90% 이상의 정상 URL 및 80% 이상의 비정상 URL의 위조 여부를 정확히 판별할 수 있음을 보였다.

본 논문의 구성은 이와 같다. 2장에서는 기존 탐지기법과의 차이점을 분석하며, 3장에서는 인터넷 주소 등

본 연구는 2013학년도 서울여자대학교 컴퓨터과학연구소 교내학술연구비의 지원을 받아 수행되었습니다.
* 서울여자대학교 정보보호학과 학사과정 (kangj1010@naver.com)
** 서울여자대학교 정보보호학과 학사과정 (grape4922@naver.com)
*** 서울여자대학교 정보보호학과 조교수, 교신저자 (sihyunglee@swu.ac.kr)

록기관에 기반한 악성 URL 탐지 기법을 제안한다. 4장에서는 총 44개 URL을 대상으로 제안된 기법의 정확도를 평가한 결과를 제시하며, 5장에서는 결론을 맺는다.

Ⅱ. 문제 정의 및 기존 대응방안

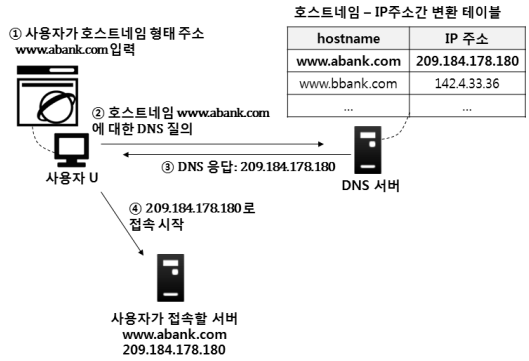
본 장에서는 먼저 해결하고자 하는 문제를 정의한 후 (2.1 절), 정의한 문제를 해결하는 기존 기법들을 본 논문에서 제안하는 기법과 비교 기술한다 (2.2절).

2.1 문제 정의

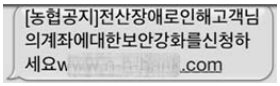
스마트기기 또는 PC 사용자가 금융거래 관련 사이트 Wu에 접속시에는 다양한 개인정보 및 주요 정보를 입력한다. 만약 공격자가 Wu 를 가장한 피싱 사이트 Wf를 설치한 후, 사용자가 Wf에 대신 접속하도록 유도한다면, 사용자가 입력한 정보는 고스란히 공격자의 손에 들어가 악의적인 목적에 사용될 수 있다. 이와 같이 사용자가 피싱 사이트 Wf에 접속하도록 유도하는 방법은 (i)접속지 호스트네임의 변조, (ii)접속지 IP 주소의 변조가 있다. 먼저 2.1.1 절에서 두 기법 모두와 관련된 DNS 프로토콜에 대해 기술한 후, 2.1.2 ~ 2.1.3 절에서 두 기법을 각각 기술한다.

2.1.1 DNS: 호스트네임과 IP주소간 변환

웹 사이트 접속시 사용자는 숫자 형태의 IP 주소를 직접 목적지 주소로 사용하기보다는 (예) 209.184.178.180), 이보다 기억하기 쉬운 문자 형태의 호스트네임 형식을 더 높은 빈도로 사용한다 (예) www.abank.com). 호스트네임 형태의 주소가 입력되는 경우 웹 브라우저의 동작 과정이 그림 1에 나타나 있다 - 먼저 (i) DNS (Domain Name Service) 프로토콜의 질의를 서버로 전송해 대응하는 IP 주소를 응답으로 받은 후, (ii) 받은 IP 주소를 목적지 IP 주소로 사용하여 접속을 시작한다. 이와 같은 접속 과정을 고려할 때, 사용자가 피싱 사이트 Wf에 접속하도록 유도하기 위해서는, (a) 단계 ①에서 사용자가 피싱 사이트에 대응되는 호스트네임을 사용하도록 변조된 URL을 제공하거나 (2.1.2절), (b) 단계 ④에서 피싱 사이트에 대응되는 IP 주소를 사용하도록 변조된 IP를 제공할 수 있다 (2.1.3절).



〔그림 1〕 DNS 프로토콜을 통해 호스트네임을 IP 주소로 변환 후 웹서버에 접속하는 과정



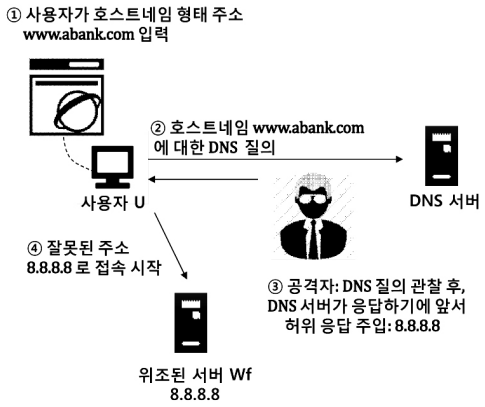
〔그림 2〕 허위 URL을 포함한 메시지 예

2.1.2 접속지 호스트네임의 변조

그림 1, 단계 ①에서 사용자가 피싱 사이트에 대응되는 호스트네임 Wf을 사용하도록 유도하기 위해서는 Wf 를 포함한 메시지를 SMS 메시지, 이메일 등으로 전송하거나 소셜 네트워킹 사이트에 포스팅하는 방법 등이 사용된다. 메시지의 내용은 사용자가 높은 확률로 Wf를 클릭하도록 다양한 사회공학적 기법(Social Engineering)을 활용해 구성되며, 그림 2와 같이 특정 은행 B를 사칭하고, B의 URL와 매우 유사한 허위 URL을 제공하며, 마치 B의 전자우편에서 보내진 것 처럼 위조하기도 한다.

2.1.3 IP주소(접속지)의 변조

그림 1, 단계 ④에서 사용자가 피싱 사이트 Wf에 대응되는 IP 주소를 사용하도록 유도하기 위해서는 전송되는 DNS 질의에 대해 피싱 사이트에 대한 IP 주소를 받도록 DNS 응답의 조작이 필요하다. 이를 위해서 먼저 ARP Spoofing 등의 네트워크 스니핑 기법을 통해 사용자가 DNS의 패킷을 전송하는 것이 관찰되면 즉시 Wf의 IP 주소를 담은 허위 DNS 응답을 주입한다 (그림 3). 사용자의 웹 브라우저상에는 접속지의 호스트네임이 표기되므로, 정상적인 사이트에 접속하는 것으로 착각하게 된다. 네트워크 스니핑에 기반하지 않고 DNS



〔그림 3〕 허위 DNS 응답 주입 (DNS 스푸핑)과정

서버를 직접 해킹하여 호스트네임-IP주소간 매핑 테이블을 조작하는 것도 허위 IP 주소가 반환되도록 조작하는 한 가지 방법이다.

사용자가 Wf의 IP 주소를 사용하도록 유도하기 위한 또 다른 방법은 사용자 기기 내의 hosts 파일을 변조하는 방법이다. Hosts 파일은 호스트네임과 대응되는 IP 주소가 리스트 형태로 저장되어 있으며, DNS 질의에 앞서 참조되는 local DNS table 이다. Hosts 파일의 변조는 주로 악성코드에 의해 이루어진다.

2.2 기존 대응방안

기존의 피싱 탐지 기법들이 본 논문에서 제안하는 Whois 기반 기법과 어떤 차이점과 유사점이 있는지 비교 분석한다.

2.2.1 제3의 인증기관을 통한 검증

현재 사용자가 접속하고 있다고 생각하는 사이트 Wu가 실제 접속하는 웹 서버 Wc와 동일함을 검증하는 한 가지 방법은, Wc가 직접 사용자에게 Wc=Wu임을, 즉 위조된 사이트가 아님을 증명하는 것이다. 이러한 증명은 Wc 가 독자적으로 하는 경우 위조 가능하기 때문에, 사용자가 신뢰할 수 있는 제 3의 인증기관 (TTP, Trusted Third Party) 이 함께 Wc 의 진위여부를 검증해 준다 [2].

TTP를 통한 증명 과정은 (i) Wc가 임의의 문서를 자신의 사설키로 전자서명하여 사용자에게 전송하면, (ii) 사용자는 TTP에게 받은 Wc의 공개키로 전자서명을 확인함으로써 이루어진다.

위의 인증 방법은 접속하는 사이트가 TTP의 인증을 받아야만 사용할 수 있으나, 인증 절차에 소요되는 시간과 비용 등으로 인해 모든 사이트가 자발적으로 TTP의 인증을 받는다고 가정하기는 어렵다. 따라서 인증절차를 거치지 않은 사이트의 위조를 검증하기 위해서는, 이어 설명할 리스트 기반, 구글 검색 기반 및 Whois 기반 검증 방법이 보완책으로 사용될 수 있다.

2.2.2 리스트기반 검증

리스트 기반 검증에서는 기존에 보고된 피싱 사이트의 URL들을 포함해 블랙리스트(Blacklist) L_B를 생성한 후, L_B에 포함된 URL로 접속이 일어난다면 피싱으로 판단한다 [2]. 블랙리스트와 반대 개념으로, 화이트리스트(Whitelist) 기반 탐지 기법도 존재한다. 피싱 공격의 목표가 될 수 있는 사이트들의 URL 및 IP 주소로 리스트 L_W를 구성한 후, L_W에 주어진 URL이나 IP 주소로 접속이 일어나는 경우 안전하다고 판단한다. 화이트리스트 기반 탐지 기법은 일반적으로 블랙리스트와 함께 사용된다.

리스트 기반 탐지기법은 리스트에 포함된 URL에 대해서는 빠짐없이 검증 가능하나, 리스트에 미처 추가되지 않은 새로운 URL은 검증하지 못한다. 따라서, 관리자는 변경 사항 발생 시마다 리스트를 주기적으로 업데이트하여 최신 정보를 유지할 필요가 있다. 이에 반해 Whois 기반 탐지 기법은 데이터베이스 업데이트에 필요한 비용이 상대적으로 낮다. 이는 Whois 데이터베이스가 외부 기관에 의해 업데이트되며 (IANA), 변경 주기가 상대적으로 길기 때문이다 (한 번 등록된 정보는 평균적으로 수 개월 이상은 동일값 유지).

2.2.3 검색엔진 기반 (구글)

앞의 두 기법의 단점을 보완할 수 있는 한 가지 방법으로 Google 검색 결과를 활용한 탐지 기법이 있으며 [3], (i) 입력 메시지 M 내에서 키워드 K를 추출한 후, (ii) K를 Google 검색하여 얻은 결과 중 상위 10개 결과에 해당하는 URL U_G를 (iii) M 내에 주어진 URL U_M과 비교하여, $U_G \neq U_M$인 경우 피싱의 가능성이 있

다고 판단한다.

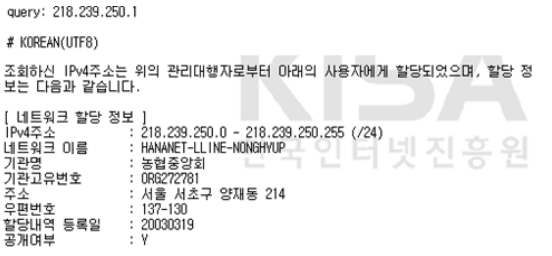
Google 기반 탐지 기법은 Google의 방대한 검색 결과를 활용하므로, 다른 기법에 비해 검증 가능한 경우가 상대적으로 광범위하다. 즉, TTP에 인증되지 않은 사이트뿐 아니라, 리스트에 추가되지 않은 사이트도 Google 검색 결과에 포함되어 있는 한 검증 가능하다. 하지만 다음과 같은 두 가지 문제점이 있으며, 본 논문에서 제안하는 Whois 기반 검증이 함께 사용된다면 이와 같은 문제점을 보완 할 수 있다. 첫째, DNS 스푸핑 공격시에는 접속 URL U가 정상 사이트 주소로 검증되더라도, 사용자는 여전히 피싱 사이트에 접속 할 수 있다. Google 기반 탐지는 U의 진위 여부만을 검증하나, DNS 스푸핑 공격은 이에 대응하는 IP 주소를 조작하기 때문이다. 반면 Whois 기반 탐지는 DNS 질의 후 반환되는 IP 주소의 진위여부를 소속 기관명을 통해 검증함으로써, IP 주소 변조 시도도 탐지 가능하다. Google 기반 탐지의 두 번째 문제는 Google의 상위 검색 결과가 항상 정확한 정보를 제공하지는 않는다는 것이다. 예를 들어, 사이트 주소가 변경될 수도 있으며, 공격자가 고의적으로 피싱 사이트의 URL을 검색 상위 랭킹에 포진할 수 있는 방법도 존재한다 [3]. 이러한 경우, Whois 데이터베이스를 함께 참조함으로써 탐지 정확도를 향상할 수 있다.

Ⅲ. 주소등록기관을 통한 URL 검증 방법

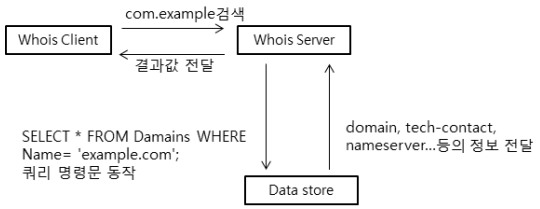
본 장에서는 2.2절에서 기술된 기존의 탐지 솔루션들을 보완하여 2.1절에 제기된 문제들을 해결할 수 있는 인터넷 주소 등록기관을 통한 접속지 검증 기법을 제안한다.

3.1 주소등록기관 및 WHOIS 데이터베이스

WHOIS는 네트워크 정보 센터 (NIC)가 관리하고 있는 통신만에 관한 정보 제공 서비스로 전 세계 각 기관들이 할당 받은 (i) IP 정보 및 등록한 (ii) 호스트네임 정보를 관리한다 (예) 1.1.1.0/24 및 호스트네임 c.security.com 은 국가 N의 기관 C에 할당됨) [5]. 이러한 등록정보는 등록 지역에 따라 서로 다른 등록기관에 분산되어 저장, 관리된다. 예를 들어 아시아에서 등록한 정보는 APNIC 에서, 아프리카에서 등록한 정보는



〔그림 4〕 Whois 응답의 예 (한국, 농협중앙회 소속)



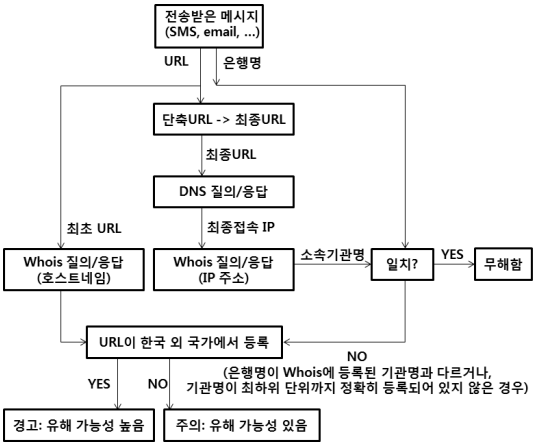
〔그림 5〕 Whois 동작원리

AfriNIC에서 관리를 담당한다. WHOIS 서버에 질의함으로써 IP 주소나 호스트네임이 등록된 국가, 기관, 관리자 연락처 등 통신망에 관한 다양한 정보를 알 수 있다. 그림 4는 WHOIS 응답의 예를 보여주며, 특히 218.290.250.0/24 대역이 농협중앙회에 할당되었음을 보여준다. 응답내의 주소로부터 이 기관이 한국에 위치함도 알 수 있다.

그림 5는 Whois 의 동작원리를 도식화 한 것이다: ① Whois 서비스를 이용하여 클라이언트가 해당 웹사이트에 대한 호스트네임이나 IP 주소를 검색하면 서버쪽으로 질의가 전송되며, ② 질의를 받은 Whois 서버는 Whois 데이터베이스에 쿼리를 실행하게 된다. ③ 데이터베이스에서 찾은 해당 도메인 또는 IP 정보 (도메인 네임, 국가, 지역, 관리자 등)가 서버에게 전달되면, ④ 정보를 전달받은 서버는 클라이언트에게 결과값을 전달한다. 일반적으로 Whois 쿼리는 1-20초 정도의 응답시간을 가지며, 일반적인 분석 시스템이나 대량의 쿼리를 요구하는 경우에는 Whois 정보를 로컬 데이터베이스에 저장함으로써 초당 1,000번 이상의 쿼리가 가능하다.

3.2 악성 URL/IP 탐지 방법

본 장에서는 제안하는 악성 URL/IP 의 구조 및 동작 순서에 대해 설명한다 (그림 6). 먼저 피싱 여부를 확인하기 위해서 수신된 메시지에 포함되어있는 웹 주소 W



〔그림 6〕 악성 URL/IP 탐지 단계

와 특징이 되는 단어 S (예) 은행명) 를 추출한다. DNS 질의응답을 통해 W에 대응되는 IP 주소를 얻을 수 있으며, 이를 Whois 데이터베이스에 질의함으로써 등록 기관명 O를 도출 할 수 있다. 마지막으로, S=O인 경우 피싱 가능성이 낮은 것으로 판단한다.

만약 S≠O인 경우 악성 URL일 가능성이 있는 것으로 판단하고 추가 검증과정을 진행한다. 최초 제공된 웹 주소 W의 등록 기관을 Whois 데이터베이스에 질의하여, 등록 국가를 확인하며, 등록 국가가 한국 이외의 지역인 경우 악성의 가능성이 높은 것으로, 그렇지 않은 경우 악성의 가능성이 상대적으로 낮은 것으로 판명한다.

① **웹주소, 특징단어 추출**: 수신된 메시지에서 먼저 웹 주소를 추출하며, 이를 위해 정규표현식 (regular expression)을 활용한다. 웹 주소는 “http://”, “https://”, “www.” 로 시작하여, 마침표 (.)로 구분된 스트링이 차례로 나타나며, 공백(\s) 이나 메시지의 끝을 나타내는 Null 문자(\0) 로 끝맺는다. 웹 주소 외에도 검증할 기관명을 추출한다. 기관명은 정규표현식 정규표현식 “.*은행”을 활용해 추출한다.

② **단축URL의 경우 원래의 웹 주소 복원**: 추출한 웹 주소가 단축 URL이라면 이를 통해 최종적으로 연결되는 (단축 URL이 아닌) 웹 주소를 복원한다. 복원을 위해서는 먼저 HTTP 요청 (GET) 메시지를 단축 URL이 가르키는 주소로 전송하며, 이때 돌아오는 응답 내에 최종적으로 연결되는 웹 주소가 포함되어 있다. 상세한 과정은 3.3 절에서 기술한다.

③ **웹 주소를 IP 주소로 변환**: 최종 목적지의 웹 주소가 가리키는 호스트의 IP 주소를 얻으며, 이를 위해 DNS 프로토콜의 질의, 응답을 활용한다.

④ **WHOIS 질의응답 (IP 주소)**: 최종 목적지의 IP 주소를 Whois 서버에 질의하여 소속 기관에 대한 정보를 얻는다. Whois 서버로부터 돌아오는 응답에서는 특히 악성 URL 여부와 가장 연관 있는 등록 기관명 및 국가를 추출하여 사용자에게 제공한다. 등록 기관명은 ‘기관명:’, ‘Organization Name:’, ‘OrgName:’ 뒤의 스트링에서 추출하며, 등록 국가명은 ‘Country:’ 뒤의 스트링에서 추출한다. 만약 소속 국가명도 함께 추출한다. 만약 추출한 등록기관명이 단계 ①에서 추출한 기관명과 일치한다면 무해함으로 판명한다. 일치하지 않는다면 단계 ⑤의 추가검사를 거쳐 악성 여부를 판명한다.

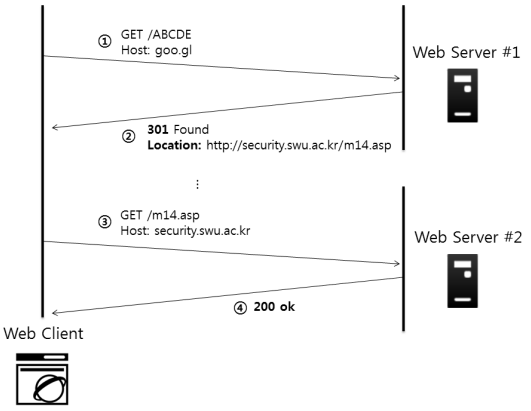
⑤ **WHOIS 질의응답 (호스트네임)**: 최종 접속지 IP의 등록기관명이 전송받은 메시지의 등록기관명과 정확히 일치하지 않는 경우 100% 유해함을 확신하기는 어렵다. 검사한 IP 주소가 WHOIS 데이터에 정확히 등록되지 않았거나, 해당 기관의 서버가 다른 서비스 제공자의 네트워크에서 운영되는 경우도 있기 때문이다. 악성일 경우를 판별하기 위해 추가로 WHOIS 질의를 하며, 특히 수신된 메시지에 실려온 최초 URL의 등록 국가를 조사한다. 등록 국가가 한국 이외인 경우 악성일 가능성이 높은 것으로 판명한다. 악성 URL 판명에 등록 국가를 활용하는 이유는, 악성으로 신고된 다수의 URL이 한국 이외의 국가에서 등록되었기 때문이다 (4.2절 참조).

3.3 단축 URL로부터 최종 목적지 웹 주소 복원법

단축 URL의 경우 그림 7과 같이 두 번 이상의 HTTP 요청, 응답 과정을 거쳐 최종 목적지에 접속한다.

① 단축 URL ‘goo.gl/ABCDE’ 로 HTTP 요청 (GET)을 전송한다.

② 최종목적지의 URL ‘security.swu.ac.kr’을 실은 응답이 돌아온다. 접속지 서버 (Web Server #1) 은 최종 목적지가 아니므로, 응답은 ‘200 OK’가



〔그림 7〕 단축 URL 사용시 최종 목적지에 접속하는 과정

아닌 '30*' 코드를 지니며, 이 때 'Location:' 필드 뒤에 최종목적지의 URL이 실린다.

③ 단계 ②에서 얻은 최종목적지 URL로 다시 HTTP 요청 (GET)을 전송한다.

④ 접속지 서버 (Web Server #2)가 최종 목적지이며, 현재 서버에 존재하는 페이지를 요청하였다면 응답으로 '200 OK'가 돌아온다. 이 때, '30*' 코드가 돌아오는 경우도 있으며 (단축 URL을 재귀적으로 여러 단계에 걸쳐 생성한 경우), 이러한 경우 단계 ②로 돌아가며, '200 OK' 응답이 돌아올 때까지 단계 ②~④를 반복한다.

Ⅳ. 주소등록기관을 통한 검증의 정확도 평가

본 장에서는 주소등록기관을 통한 검증의 정확도를 12개 정상 URL 및 32개 악성 URL을 대상으로 평가하였으며, 정상 URL의 경우 90% 이상의 정확도로, 악성 URL의 경우 80% 이상의 정확도로 판별해 낼 수 있음을 보았다. 정상 URL 샘플로 국내 12개 은행 사이트의 URL을 사용하였으며, 악성 URL 샘플로는 피해사례로 보고된 24개 URL을 사용하였다 [9].

4.1 최종접속 IP를 이용한 정상URL검증의 정확도

국내 12개 은행 사이트를 대상으로 최종 접속 IP주소의 등록기관을 확인해 보았으며, 90% 이상의 정확도로 정상 여부를 판별해 낼 수 있음을 검증할 수 있었다. 정확도 평가 방법은 다음과 같다.

① 12개의 평가 대상 사이트는 Google 검색 엔진에서 키워드 '은행' 으로 검색하였을 때, 상위로 검색되는 사이트들로 선정되었다.

② 각 평가 대상 사이트 S의 (변조되지 않은) URL을 구현된 시스템에 입력으로 사용하여, 출력으로 기관명 O를 얻는다.

③ 만약 ②의 결과로 얻은 O가 S의 기관명과 일치한다면 탐지 시스템은 S에 대한 피싱 가능성을 탐지할 수 있음을 의미한다. 즉, (i) 호스트네임 또는 IP 주소가 변조되지 않았다면 O와 S가 일치함으로써 변조되지 않았음을 판명 가능하며, (ii) 호스트네임 또는 IP 주소가 S 이외의 장소로 변조되었다면 (예) 중국, 인도에 위치한 서버), 탐지 시스템의 출력 O'는 S와 일치하지 않을 것이며, 이로부터 변조 가능성을 판명할 수 있기 때문이다.

④ 만약 ②의 결과로 얻은 O가 S와 일치하지 않는다면 탐지 시스템은 S에 대한 피싱 가능성을 탐지하기 어려움을 의미한다. 즉, (i) 호스트네임 또는 IP 주소가 변조되지 않은 경우에도 O는 S의 기관명이 일치하지 않고, (ii) 호스트네임 또는 IP 주소가 S 이외의 장소로 변조된 경우에도, 탐지 시스템의 출력 O'는 S와 일치하지 않게 되어, 결국 (i), (ii) 두 가지 경우를 구분할 수 없기 때문이다.

①~④ 에 따른 평가 결과, 12개 은행 사이트 중 11개 사이트에 대해 위의 ③에 해당하는 결과, 즉 제안된 시스템을 사용해 '피싱 가능성을 탐지할 수 있음'을 알 수 있었다. 또한, 두 사이트에 대해서는 Whois를 통해 얻은 기관명이 실제 기관명과 정확히 일치하지는 않으나 피싱 가능성 판별에 도움이 되는 정보를 제공함을 볼 수 있었다 (우리카드 ⇨ 한빛은행, 신한카드 ⇨ LG카드). 다만, 한 사이트에 대해서는 판별에 도움되는 정보를 얻을 수 없었다 (하나은행 ⇨ KT [1]). 표 1에 평가에 사용된 12개 은행 사이트에 대한 결과를 요약하였다.

1) '하나은행'의 경우 Whois 결과값의 기관명으로 '하나은행'을 얻을 수 없었으며, 하나은행에 인터넷 접속을 제공하는 ISP가 KT임만을 알 수 있었다. 하나은행에 대한 IP 주소 할당정보가 Whois 데이터베이스에 정확히 업데이트되어있지 않은 것으로 추정된다.

〈표 1〉 국내 대표 은행 사이트의 등록기관 검증 결과

은행명	URL	등록 기관명 (WHOIS 질의결과 中)
우리은행	www.wooribank.com	한빛은행
신한은행	www.shinhan.com	신한은행
국민은행	www.kbstar.com	㈜국민은행본점
농협	www.nonghyup.com	농협중앙회
기업은행	www.ibk.co.kr	중소기업은행
하나은행	www.hanabank.com	주식회사 케이티
외환은행	www.keb.co.kr	한국외환은행
대구은행	www.dgb.co.kr	㈜대구은행
부산은행	www.busanbank.co.kr	㈜부산은행
한국시티은행	www.citibank.co.kr	Citicorp Global Information Network
한국산업은행 = KDB 산업은행	www.kdb.co.kr	한국산업은행
HSBC 은행 서울지점	www.kr.hsbc.com	HSBC banking and financial services

4.2 URL등록국가를 활용한 악성URL검증의 정확도

추가적으로, 위조 가능성이 있는 URL도 Whois 데이터베이스를 통해 소속정보를 확인해 보았다. 피해정보 사이트에 악성으로 보고된 주소 중 표 1에 나열된 기관을 언급한 32개 URL의 등록 국가를 WHOIS 데이터베이스를 통해 확인 해 보았다. 확인 결과, 27개의 URL (84.4%) 이 중국, 인도를 포함한 국외에서 등록되었음을 확인할 수 있었다. 이들의 등록기관 역시 표 1에 나열된 등록기관이 아니었다. 즉, 제안된 방법을 통해 악성임을 판명 가능했다.

평가 결과를 요약하면, 현존하는 은행 사이트에 대해 8-90% 이상의 정확도로 피싱 여부를 탐지할 수 있음을 검증할 수 있었다. 즉, 제안된 탐지기법을 활용하면 IP 변조 공격이 진행되는 경우에도 기존 탐지기법들(2.2절)에 비해 피싱 사이트에 접속할 가능성을 크게 감소시킬 수 있다.

제안된 Whois기반 탐지 기법의 또 다른 장점은, 등록·인증과정 없이 개방되어 사용가능한 Whois 및 DNS 서비스에 기반하므로, 제3의 인증기관을 통한 탐지에 비해 등록·인증에 소요되는 시간, 비용을 크게 줄일 수 있다. 또한, Whois 데이터베이스는 외부 등록 기관에 의해 관리되므로, 리스트기반 검증과 같이 사용자가 데이터베이스를 이를 주기적으로 업데이트하는 수고를 덜 수 있다.

Ⅴ. 결 론

본 논문에서는 악성 URL 탐지를 위해 URL의 등록

〈표 2〉 악성으로 보고된 URL의 등록 국가 검증 결과

등록 국가 (WHOIS 질의결과 中)	URL
중국	zxbank.com, WTM79.com CKB17.com, hjhj77.com marry866.com, market02.org www.kbhnbank.com any133.org, is.gd/AWHKEz www.nh-tpbank.com kbssar.com, kbsncard.com axx78.com, kma38.com new-world58.com, cdd33.com hge85.com
미국	h-bank.com, tiny.cc/jex3uw nuna.us/allyak, cc56.net
태국	nh-ycbank.com, nh-ucbank.com
필리핀	zozo933.com, www.kss99.com
타이완	doiop.com/8bk36b
일본	bt-82.com
한국	Avc6.com, h2002a.com 2u.lc/BOp3, now-79.com infocap.kr/4d404d61bb4ec396

기관 및 주소를 검증하는 방법을 제시하였다. 이를 위해, 인터넷 주소 등록기관의 WHOIS 데이터베이스를 활용한다. 제시된 방법은 수신된 메시지 내의 웹 주소와 WHOIS의 결과로 얻은 등록기관명, 등록국가명을 비교하여, 악성 URL 여부를 판단한다. 현재 제안된 방법을 Android 및 PC 환경에서 구현 중에 있으며, 웹 주소가 담긴 메시지를 사용자가 열람함과 동시에 메시지에서 추출된 정보를 whois정보와 비교하고, Toast기능 등을 통해 악성 URL일 가능성을 미리 알려주어 접속을 방지할 계획이다. Whois 기반 탐지는 기존대응방안에서 수행하는 호스트네임의 변조 여부에 대한 검사뿐 아니라, 최종적으로 접속이 일어나는 IP 주소에 대한 변조 검사

도 동시에 수행함으로써, 호스트네임 및 IP의 변조 모두를 탐지한다는 장점이 있다. 반면, Whois 데이터베이스는 소규모 기관의 기관명까지 항상 명확히 제공해주지는 않으므로, 중간규모 이상의 기관 (예) /28 또는 이보다 큰 주소를 할당받은 기관) 에 대한 주소 변조 탐지에 사용이 제한될 수 있다. 따라서 Whois 데이터베이스를 이용한 탐지기법에 기존 대응방안인 검색엔진(구글)기반의 대응방안을 접목시킨다면 좀 더 효과적으로 대응할 수 있을 것으로 예측된다.

참고문헌

[1] 이상일 기자, “모바일뱅킹 확산, 스마트폰이 확실한 견인차“, 디지털 데일리, 2011-08-01 http://www.ddaily.co.kr/news/news_view.php?uid=80823

[2] 민동옥, 손태식, 문종섭, “URL 스푸핑을 이용한 피싱 공격의 방어에 관한 연구,” 情報保護學會論文誌 Vol.15 No.5, 35~45쪽, 2005.

[3] 이민수, 이형규, 윤현수, “검색 엔진 기반의 안티 피싱 기법,” 한국컴퓨터종합학술대회 논문집, Vol.37, No.1(D), 2010.

[4] 사준호, “피싱사이트 실시간 탐지 기법,” 정보보호학술논문지, 제2권 제4호, p819~825, 2012.

[5] Stephane Bortzmeyer, “The Whois Serverice”, http://www.generic-nic.net/sheets/practical/whois-en

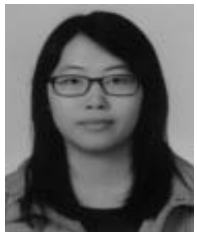
[6] Google Guava Library http://code.google.com/p/guava-libraries/

[7] Apache HTTPComponents Library http://hc.apache.org/

[8] Whois기반 피싱탐지 프로토타입 코드 http://sites.google.com/site/sihyungleeweb/home/codes-for-phishing-detection

[9] 소액결제 피해 신고 사이트 OTTL http://m.ottl.co.kr/index.ottl

〈저자소개〉



강 지 윤 (Ji Yoon Kang)
2011년 3월~현재 : 서울여자대학교 정보보호학과
<관심분야> 네트워크, 정보보호

조 은 정 (Eun Jeong Cho)
2011년 3월~현재 : 서울여자대학교 정보보호학과
<관심분야> 네트워크, 정보보호

이 시 형 (Sihyung Lee)
2010년 5월 : 카네기멜론대학교전자컴퓨터공학과 박사
2010년 7월~2011년 8월 : IBM 왓슨 연구소 박사후연구원
2011년 9월~현재 : 서울여자대학교 정보보호학과 조교수
<관심분야>: 컴퓨터 네트워크, 네트워크 관리 및 보안